



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Se

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/944,961	08/30/2001	Masashi Kon	09792909-5129	2225

7590 03/23/2005

Sonnenschein, Nath & Rosenthal
P.O. Box #061080
Wacker Drive Station - Sear Tower
Chicago, IL 60606

EXAMINER

ELMORE, JOHN E

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 03/23/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/944,961

Applicant(s)

KON ET AL.

Examiner

John Elmore

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 30 August 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-24 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-24 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 30 August 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-24 have been examined.

Objections to Specification

2. **Claim 12 is objected to** because of the following informalities: the term "any one of" (line 2) should be followed by a colon (i.e. "any one of:"). Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. **Claim 12 is rejected under 35 U.S.C. 112, second paragraph**, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The phrase "such as" (lines 3 and 6) renders the claim indefinite because it is unclear whether the limitations following the phrase are part of the claimed invention. See MPEP § 2173.05(d). In the interest of compact prosecution, the limitations following the phrase "such as," and ending with a semicolon, subsequently are ignored.

Also, the term "a card" (line 7) in claim ¹²~~10~~ is a relative term which renders the claim indefinite. The term "a card" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the gr.

art would not be reasonably apprised of the scope of the invention. In the interest of compact prosecution, this limitation subsequently is ignored.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1, 2, 6, 8, 10, 12, 13, 14, 18, 20, 22, and 24 are rejected under 35

U.S.C. 102(e) as being anticipated by Dulude et al., hereafter Dulude (US 6,310,966).

Regarding claim 1, Dulude discloses an information processing apparatus that executes person authentication by comparing a template (registration biometric data) acquired from a person identification certificate storing a template (biometric certificate 68) which is person identification data of a user using said information processing apparatus with sampling information input (transaction biometric data) by the user (col. 7, lines 33-44), and

performs connection to said external server (col. 8, lines 1-7) provided that said person authentication is successfully passed.

Regarding claim 2, Dulude all the limitations of claim 1, and further teaches that said information processing apparatus stores a person identification certificate in a memory provided in said information processing apparatus (col. 5, lines 33-41).

Regarding claim 6, Dulude all the limitations of claim 1, and further teaches that wherein said information processing apparatus forms a link in which a person identification certificate and a public key certificate applied during a process of establishing a connection for data communication with a party is related to each other, and stores the link in a storage means thereof (private key 36; public key 70; col. 4, lines 61-65; col. 5, lines 33-41; col. 6, lines 58-65).

Regarding claim 8, Dulude all the limitations of claim 1, and further teaches that said information processing apparatus downloads a person identification certificate applied to person authentication from a person identification certificate authority (registration authority 34) which is an entity for issuing a person identification certificate and stores the downloaded person identification certificate, wherein, when there is a public key certificate applicable to a process relating to application of the person identification certificate acquired by downloading, said information processing apparatus updates link information in which said person identification certificate and said public key certificate are related to each other, and stores said person identification certificate and said public key certificate in a memory provided in said information processing apparatus (biometric identification and public key certificate are combined as a biometric certificate 38; private key 36; public key 70; Fig. 2; col. 3, lines 32-34; col. 4, lines 15-20 and 55-65; col. 5, lines 33-49; col. 6, lines 59-62).

Regarding claim 10, Dulude all the limitations of claim 1, and further teaches that said information processing apparatus downloads a public key certificate from a certificate authority which is an entity for issuing a public key certificate and stores the downloaded public key certificate in a storage means thereof, and wherein, when there is a person identification certificate applicable to a process relating to application of the public key certificate acquired by downloading, said information processing apparatus updates link information in which said person identification certificate and said public key certificate are related to each other, and stores said person identification certificate and said public key certificate in a memory provided in said information processing apparatus(private key 36; public key 70; Fig. 2; col. 3, lines 32-34; col. 4, lines 15-20 and 55-65; col. 5, lines 33-49; col. 6, lines 58-62).

Regarding claim 12, Dulude all the limitations of claim 1, and further teaches that said template is composed of any one of: biometric information of a person; non-biometric information; any combination of two or more of said biometric information and said non-biometric information; and a combination of any of said information and a password (registration biometric data; col. 4, lines 15-36).

Regarding claims 13, 14, 18, 20, 22 and 24, these a method version of the claimed apparatus discussed above (claims 1, 2, 6, 8, 10 and 1, respectively), wherein all claim limitations have been addressed. Thus, for the reasons provided above, such claims also are anticipated.

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. **Claim 3, 7, 9, 11, 15, 19, 21 and 23 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Duluth in view of Diffie et al., hereafter Diffie ("Authentication and Authenticated Key Exchanges," Designs, Codes and Cryptography, Kluwer Academic Publishers, 1992).

Regarding claim 3, Duluth teaches all the limitations of claim 1, and further teaches that said information processing apparatus holds link information in which a person identification certificate and a public key certificate applied during a process of establishing a connection to said external server are related to each other and stores the person identification certificate and the public key certificate in a memory provided in said information processing apparatus and wherein said information processing apparatus extracts the public key certificate linked to said person identification certificate on the basis of the link information, provided that personal authentication on the basis of said person identification certificate is successfully passed (col. 4, lines 61-65; col. 6, lines 58-65).

But Duluth does not explain that said information processing apparatus performs mutual authentication between said external server and said information processing apparatus by applying the extracted public key certificate.

However, Diffie teaches a method of two-party mutual authentication wherein the parties exchange digital signatures (page 9, first paragraph) with their public cryptographic keys for the purpose of enhancing security by assuring that each of the parties exchanging a public key is authentic and not an imposter (page 2, paragraph 3).

Therefore, it would be obvious to a person of ordinary skill in the computer art at the time the invention was made to modify the system of Duluth with the teaching of Diffie such that said information processing apparatus performs mutual authentication between said external server and said information processing apparatus by applying the extracted public key certificate. One would be motivated to do so in order to enhance network security by assuring that each of the parties exchanging a public key is authentic and not an imposter.

Regarding claim 7, Duluth teaches all the limitations of claim 1, and further teaches that said information processing apparatus downloads a person identification certificate applied to person authentication from a person identification certificate authority (registration authority 34) which is an entity for issuing a person identification certificate and stores the downloaded person identification certificate in a storage and means thereof (col. 4, lines 15-20; col. 5, lines 33-49).

But Duluth does not explain that, in a process of downloading said person identification certificate, apparatus performs mutual authentication between said information processing apparatus and said person identification certificate authority, and downloads the person identification certificate from said person said information

Art Unit: 2134

processing authentication between said identification certificate authority provided that said mutual authentication is successfully completed.

However, Diffie teaches a method of two-party mutual authentication wherein the parties exchange digital signatures (page 9, first paragraph) with their public cryptographic keys for the purpose of enhancing security by assuring that each of the parties exchanging a public key is authentic and not an imposter (page 2, paragraph 3).

Therefore, it would be obvious to a person of ordinary skill in the computer art at the time the invention was made to modify the system of Duluth with the teaching of Diffie such that, in a process of downloading said person identification certificate, apparatus performs mutual authentication between said information processing apparatus and said person identification certificate authority, and downloads the person identification certificate from said person said information processing authentication between said identification certificate authority provided that said mutual authentication is successfully completed. One would be motivated to do so in order to enhance network security by assuring that each of the parties exchanging a public key is authentic and not an imposter.

Regarding claim 9, Duluth teaches all the limitations of claim 1, and further teaches that said information processing apparatus downloads a public key certificate from a certificate authority which is an entity for issuing a public key certificate and stores the downloaded public key certificate in a storage means thereof (private key 36; public key 70; col. 4, lines 61-62; col. 6, lines 58-62).

But Duluth does not explain that, in a process of downloading said public key certificate, said information processing apparatus performs mutual authentication between said information processing apparatus and said certificate authority, and downloads said public key certificate from said certificate authority provided that said mutual authentication is successfully completed.

However, Diffie teaches a method of two-party mutual authentication wherein the parties exchange digital signatures (page 9, first paragraph) with their public cryptographic keys for the purpose of enhancing security by assuring that each of the parties exchanging a public key is authentic and not an imposter (page 2, paragraph 3).

Therefore, it would be obvious to a person of ordinary skill in the computer art at the time the invention was made to modify the system of Duluth with the teaching of Diffie such that, in a process of downloading said public key certificate, said information processing apparatus performs mutual authentication between said information processing apparatus and said certificate authority, and downloads said public key certificate from said certificate authority provided that said mutual authentication is successfully completed. One would be motivated to do so in order to enhance network security by assuring that each of the parties exchanging a public key is authentic and not an imposter.

Regarding claim 11, Duluth teaches all the limitations of claim 1, and further teaches that said information processing apparatus includes an encryption processing unit (e.g. biometric certificate extractor 64; col. 6, lines 60-61).

But Duluth does not explain that in data transmission/reception between said information processing apparatus and said external server, performs mutual authentication between said information processing apparatus and said external server and further, a data transmitting end adds a digital data to the transmitted data and a data receiving end verifies the digital signature.

However, Diffie teaches a method of two-party mutual authentication wherein the parties exchange digital signatures (page 9, first paragraph) with their public cryptographic keys for the purpose of enhancing security by assuring that each of the parties exchanging a public key is authentic and not an imposter (page 2, paragraph 3).

Therefore, it would be obvious to a person of ordinary skill in the computer art at the time the invention was made to modify the system of Duluth with the teaching of Diffie such that in data transmission/reception between said information processing apparatus and said external server, performs mutual authentication between said information processing apparatus and said external server and further, a data transmitting end adds a digital data to the transmitted data and a data receiving end verifies the digital signature. One would be motivated to do so in order to enhance network security by assuring that each of the parties exchanging a public key is authentic and not an imposter.

Regarding claims 15, 19, 21 and 23, this is a method version of the claimed apparatus discussed above (claims 3, 7, 9 and 11, respectively), wherein all claim limitations have been addressed. Thus, for the reasons provided above, such claims also would have been obvious.

7. **Claims 4, 5, 16 and 17 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Duluth in view of Ginter et al., hereafter Ginter (US 5,892,200).

Regarding claim 4, Duluth teaches all the limitations of claim 1, and further teaches that

said external server is a contents providing server (col. 1, lines 28-36; col. 3, lines 35-36; col. 5, lines 56-58) and

said information processing apparatus executes person authentication by comparing the template extracted from said person identification certificate with sampling information input by a user, establishes a connection to the contents providing server providing that said person authentication is successfully passed, and downloads the contents (col. 7, line 33, through col. 8, line 7).

Although Duluth teaches that the information processing apparatus is a transaction processing system connecting a user with an external content provider (col. 1, lines 28-36; col. 8, lines 1-7), Duluth does not explicitly explain that said information processing apparatus is an apparatus having the function of reproducing contents.

However, Ginter teaches an information processing apparatus (VDE) connected to an external content provider (106) having the function of reproducing contents (e.g. "traveling" object; col. 24, lines 54-66) for the purpose of providing more manageable and secure content distribution (col. 3, lines 18-21).

Therefore, it would be obvious to a person of ordinary skill in the computer art at the time the invention was made to modify the system of Duluth with the teaching of

Ginter such that said information processing apparatus is an apparatus having the function of reproducing contents. One would be motivated to do so in order to provide more manageable and secure content distribution.

Regarding claim 5, Duluth teaches all the limitations of claim 1, and further teaches that said information processing apparatus

executes person authentication by comparing a template extracted from said person identification certificate with sampling information input by a user (col. 7, lines 33-44),

establishes a connection to one of said user registration server and the service registration server provided that said person authentication is successfully passed, and transmits necessary data corresponding to any one of said processes of user registration, erasure of user registration, and making a service contract to said user registration server (col. 7, line 45, through col. 8, line 7).

Although Duluth teaches that the information processing apparatus is a transaction processing system connecting a user with an external server (col. 1, lines 28-36; col. 8, lines 1-7), Duluth does not explicitly explain that the external server is one of a user registration server and a service registration server which performs any one of processes of user registration, erasure of user registration, and making a service contract to a service providing entity.

However, Ginter teaches an information processing apparatus (VDE) wherein the external server is a service registration server (clearinghouse) that makes a service

Art Unit: 2134

contract to a service providing entity (col. 5, lines 42-45; col. 36, lines 10-43) for the purpose of better managing and securing electronic transactions (col. 3, lines 18-21).

Therefore, it would be obvious to a person of ordinary skill in the computer art at the time the invention was made to modify the system of Duluth with the teaching of Ginter such that the external server is one of a user registration server and a service registration server which performs any one of processes of user registration, erasure of user registration, and making a service contract to a service providing entity. One would be motivated to do so in order to better manage and secure electronic transactions.

Regarding claims 16 and 17, this is a method version of the claimed apparatus discussed above (claim 4 and 5), wherein all claim limitations have been addressed. Thus, for the reasons provided above, such claims also would have been obvious.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Bianco et al. (US 6,256,737) discloses a user authentication system employing biometric data.

Cordery et al. (US 5,796,841) teaches a system for authentication of users for e-commerce involving digital certificates.


Deo et al. (US 5,721,781) teaches a system for mutual authentication of entities over a network by exchanging digital signatures.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to John Elmore whose telephone number is 571-272-4224. The examiner can normally be reached on M 10-8, T-Th 9-7.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on 571-272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

JE


GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2129